(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－198437

(43)公開日　平成９年(1997)７月31日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　17/60			Ｇ０６Ｆ　15/21	Ｚ	
19/00		7259－5Ｊ	Ｇ０９Ｃ　1/00	６３０Ｚ	
Ｇ０９Ｃ　1/00	６３０	7259－5Ｊ		６４０Ｄ	
	６４０	7259－5Ｊ		６６０Ｄ	
	６６０	7259－5Ｊ		６６０Ｅ	

審査請求　未請求　請求項の数２　ＯＬ　（全６頁）　最終頁に続く

(21)出願番号　特願平8－6361

(22)出願日　平成８年(1996)１月18日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　葛西　健人
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　松下　博則
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　村上　昌彦
神奈川県秦野市堀山下１番地　日立コンピュータエンジニアリング株式会社内

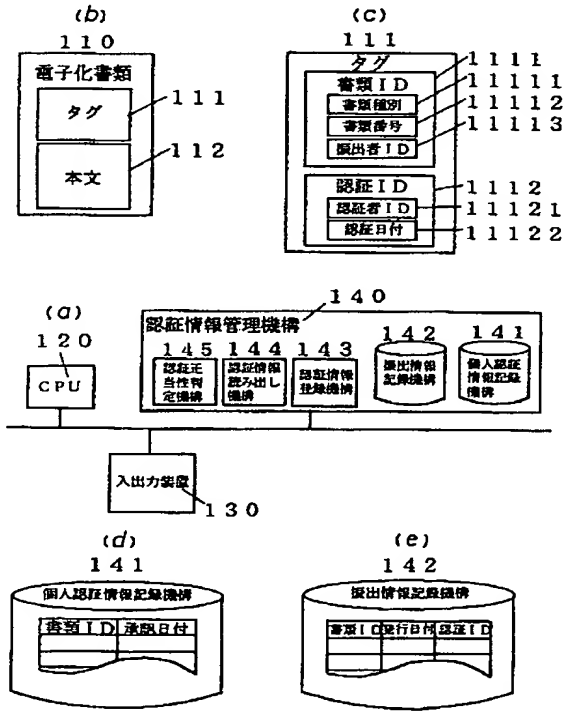
(74)代理人　弁理士　磯村　雅俊

(54)【発明の名称】　電子認証の管理方法

(57)【要約】

【課題】　電子認証において、書類の発行記録・発行した書類の記録・認証記録・最終処理の記録等の認証情報を、電子化書類と認証者の電子計算機の両方に記録し、電子化書類に付随する認証情報と、認証者の個々の電子計算機内の認証情報との整合性の確認によって、書類の発行・認証の途中経過・最終状態等の認証の正当性の判定を実施することで、認証情報の改竄の発見を容易とし、認証情報の改竄を困難とする。

【解決手段】　認証情報は、電子化書類１１０のタグ１１１に記録された認証情報と、認証者の電子計算機の個人認証情報記録機構１４１に記録された認証情報とに、分散し多重化されている。電子化書類１１０のタグ１１１の認証情報を改竄しても、電子化書類１１０のタグ１１１の認証情報と認証者の電子計算機の個人認証情報記録機構１４１に記録された認証情報とを、認証正当性判定機構１４５が整合性を確認することで簡単に改竄が発見できる。



1

【特許請求の範囲】

【請求項１】　認証者が電子計算機にて電子化書類の認証を行う方法において、

電子化書類の認証情報を当該電子化書類に付随させるとともに認証者の電子計算機に記録し、

電子化書類に付随する認証情報と認証者の電子計算機内の認証情報との整合性の確認によって、当該電子化書類の認証の正当性を判定することを特徴とする、電子認証の管理方法。

【請求項２】　認証者が電子計算機にて電子化書類の認証を行う方法において、

電子化書類の認証情報を当該電子化書類に付随させるとともに認証者の電子計算機に記録し、当該認証情報を定期的にバックアップ用の補助記録手段に複写し、

電子化書類に付随する認証情報と認証者の電子計算機内の認証情報との整合性の確認によるか、電子化書類に付随する認証情報と前記補助記録手段の認証情報との整合性の確認によって、当該電子化書類の認証の正当性を判定することを特徴とする、電子認証の管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子化書類における電子認証の管理方法において、認証情報を電子化書類と認証者の電子計算機の両方に記録することで、認証記録の改竄を困難にする方法に関する。

【０００２】

【従来の技術】

（１）従来の、電子化書類の認証の管理は、認証の印として認証者固有の印影を認証情報として記録し、これを確認する方式がある。この場合、印影の正当性は、印影使用の正当性で保証される。

（２）従来の、電子化書類の認証の管理は、認証の印としてユーザＩＤを認証情報として記録し、これを確認する方法がある。この場合、ユーザＩＤの正当性は、ユーザＩＤの使用の正当性で保証される。

（３）従来の、電子化書類の認証の管理は、電子化書類を暗号化し、鍵の設定により認証可能な認証者ををを特定することで、これを確認する方式がある。この場合、認証の正当性は、鍵の使用の正当性によって保証される。

なお、（１）特開平０２－２７８９３７号公報には、電子化書類の承認・不承認・修正の履歴をとることで、再承認作業の効率化に関する技術が記載されている。また、（２）特開平０５－２９００６６号公報には、認証の印として電子化された画像による印影を用いる方式に関する記載がある。また、（３）特開平０６－１１９３６３号公報には、電子化書類の更新権限の設定をパスワードで行う方式に関する記載がある。

【０００３】

【発明が解決しようとする課題】上記従来技術（１）は、印影使用の正当性が認証者の印影の管理に委ねられており、また、電子化された印影は複写が容易であることから、印影の盗用による認証記録の改竄が可能という問題があった。上記従来技術（２）は、ユーザＩＤおよびパスワードの正当性が認証者の管理に委ねられており、また、ユーザＩＤおよびパスワードは簡単な英数字列であることが多いため、ユーザＩＤおよびパスワードの盗用による認証記録の改竄が可能という問題があった。上記従来技術（３）は、鍵の正当性が認証者の管理に委ねられており、また、鍵は簡単な英数字列であることが多いため、鍵の盗用による認証記録の改竄が可能という問題点があった。本発明の目的は、このような問題点を改善し、認証情報の改竄の発見を容易とし、認証情報の改竄を困難とすることが可能な電子認証の管理方法を提供することにある。

【０００４】

【課題を解決するための手段】上記目的を達成するために、本発明は、分散・多重化された認証情報により電子認証を行う。すなわち、電子化書類に付随して記録された認証情報（例えば、書類の発行記録・発行した書類の記録・認証記録・最終処理の記録・書類に関係するその他の記録の認証情報）と、認証者の電子計算機に記録された認証情報またはバックアップ用の補助記録手段に複写記録された認証情報との整合性を確認することによって、書類の発行・認証の途中経過・最終状態等の認証の正当性の判定を実施する。

【０００５】

【発明の実施の形態】本発明においては、認証情報は、電子化書類に付随して記録された認証情報と、それぞれの認証者の電子計算機あるいはバックアップ用の補助記憶手段に記録された認証情報とに、分散し多重化されている。それによって、電子化書類に付随した認証情報を改竄しても、認証者の電子計算機あるいはバックアップ用の補助記憶手段に記録された認証情報との整合性を確認することで、簡単に改竄が発見できる。なお認証情報の改竄には、承認・不承認の変更、認証対象者の変更がある。

【０００６】以下、本発明の実施例の詳細を図面に基づいて説明する。図１は、本発明の一実施例の装置構成を示す図である。同図において、１１０は電子化書類、１１１はタグ、１１２は本文、１２０は装置全体を統括制御するＣＰＵ、１３０は装置へ及び装置からの入出力装置、１４０は認証情報管理機構、１４１は個人認証情報記録機構、１４２は振出し情報記録機構、１４３は認証情報登録機構、１４４は認証情報読み出し機構、１４５は認証正当性判定機構である。本実施例の電子計算機システムは、（ａ）に示す通りであって、電子化書類１１０は、（ｂ）に示すように、タグ１１１と本文１１２から構成される。タグ１１１は、（ｃ）に示すように、電子化書類に付随する認証情報で、書類を特定する書類ＩＤ１１１１および認証の対象者・認証の状態を示す認証

2

ＩＤ１１１２から構成され、書類の認証情報を記録する。書類を特定する書類ＩＤには、書類の重要度や緊急度を示す書類種別１１１１１、当該書類が一意であることを示す書類番号１１１１２、振出者ＩＤ１１１１３から構成される。発行の記録には、発行の事実および日付時間がある。認証の対象者には、氏名およびユーザＩＤがある。認証の状態を示す認証ＩＤ１１１２には、認証者を特定する認証者ＩＤ１１１２１・認証日付１１１２２から構成される。認証情報管理機構１４０は、個人認証情報記録機構１４１、振出情報記録機構１４２、認証情報登録機構１４３、認証情報読み出し機構１４４、認証正当性判定機構１４５から構成される。認証情報登録機構１４３は、電子化書類１１０が作成されると、そのタグ１１１および本文１１２に基づいて、振り出し記録を、（ｅ）に示す振出情報記録機構１４２に登録する。振り出し記録には、書類ＩＤ１１１１・発行日付および認証対象者を特定する認証ＩＤ１１１２を記録する。また、電子化書類１１０について認証が実施されると、その認証情報を個人認証情報記録機構１４１に登録する。個人認証情報記録機構１４１は、（ｄ）に示すように、認証者の電子計算機における認証者個人の認証情報記録機構で、書類ＩＤ１１１１・認証日付１１１２２を記録する。認証情報読み出し機構１４４は、認証正当性判定機構１４５の要求に基づいて、個人認証情報記録機構１４１から当該電子化書類１１０の認証情報を取り出し、当該認証正当性判定機構１４５に返す。認証正当性判定機構１４５は、当該電子化書類１１０のタグ１１１の認証情報に基づいて、当該電子化書類１１０の認証確認対象者を選定し、自動的または操作者の指示に基づいて、一部または全ての認証確認対象者の電子計算機の認証情報読み出し機構１４４に対して認証情報の提示を要求し、各認証情報読み出し機構１４４から返された認証情報と当該電子化書類１１０のタグ１１１の認証情報との整合性を確認し、認証記録の正当性を判定する。

【０００７】図２は、本発明の一実施例の電子化書類の認証と認証の確認の流れを簡単に示す図である。同図において、振り出し者２１０の電子計算機で電子化書類２２０が作成されると、電子化書類の振り出し情報が、振り出し者２１０の電子計算機の振出情報記録機構２１１と電子化書類２２０のタグ２２１に記録され、最初の認証対象者２３０の電子計算機に向けて電子化書類２２０が振り出される。電子化書類２２０が最初の認証対象者２３０の電子計算機に到達し認証された場合、その認証情報が、認証対象者２３０の電子計算機の個人認証情報記録機構２３１と電子化書類２２０のタグ２２１に記録され、電子化書類２２０が次の認証対象者２４０に回覧される。電子化書類２２０が最終判断者２５０の電子計算機に到達した場合、最終判断者２５０は当該書類のタグ２２１に記録された書類ＩＤ２２１１の書類種別で示される書類の重要度や緊急度に応じて認証の確認が必要か判断する。認証の確認が必要であると判断した場合、最終判断者２５０は最終判断者２５０の電子計算機から認証正当性の確認を行う。

【０００８】図３は最終判断者３１０の認証正当性確認処理の流れを示す図である。同図において最終判断者３１０は、最終判断者３１０の電子計算機の認証正当性判定機構３１１に対して認証確認対象者を指定して、電子化書類３２０の認証の正当性の確認を指示する。　最終判断者３１０の電子計算機の認証正当性判定機構３１１は、最終判断者３１０の指示の基づいて認証確認対象者３３０の電子計算機の認証正当性判定機構３３１に、当該書類３２０の書類ＩＤ３２１を送信し、認証確認対象者３３０が、当該書類３２０を正当に認証しているか否かを問い合わせる。書類ＩＤ３２１を受け取った認証確認対象者３３０の電子計算機は、当該電子計算機の認証正当性判定機構３３１から認証情報読み出し機構３３２に対し、当該書類ＩＤ３２１が示す書類３２０の認証情報の読み出し指示を出す。認証情報読み出し機構３３２は、個人認証情報記録機構３３３から当該書類３２０の認証情報の読み出し処理を行い、当該書類３２０の認証情報が個人認証情報記録機構３３３に登録されていた場合、認証正当性判定機構３３１に読み出した認証情報を返す。また、当該書類３２０の認証情報が個人認証情報記録機構３３３に登録されていなかった場合、認証正当性判定機構３３１に当該書類ＩＤ３２１が示す書類３２０の認証情報無しのメッセージを返す。認証確認対象者３３０の認証正当性判定機構３３１は、個人認証情報記録機構３３３から返された読み出し結果が、最終判断者３１０から受信した書類ＩＤ３２１で示す書類３２０が承認されているという場合、認証情報の承認のメッセージ３３４を最終判断者３１０の電子計算機に応答する。また、当該書類ＩＤ３２１無しの場合、または当該書類３２０は不承認であるという認証情報の場合、不承認のメッセージ３３４を最終判断者３１０の電子計算機に応答する。次に、メッセージ３３４を受けた最終判断者３１０の電子計算機は、ディスプレイ装置またはその他の出力装置により、認証確認対象者３３０の承認および不承認の情報を最終判断者３１０に提示する。最終判断者３１０は、提示された承認および不承認のメッセージに基づき、当該書類３２０に対する認証の正当性を確認、決裁の判定を行う。また、本認証の確認は最終判断者以外の認証者が、その時点での認証の正当性の判定に用いることも可能である。

【０００９】なお、本実施例では、個人認証情報記録機構に認証情報を記録しているが、この他にバックアップ用の補助記録装置を設けてもよい。あるいはその補助記録装置をデータベース化してもよい。これにより、当該認証者の電子計算機がダウンしている場合でも電子化書類の認証の正当性を判定することができる。また、最終判断者の認証判定は、電子計算機が自動的に行うように

5

してもあるいは操作者の指示により行うようにしてもよい。

【００１０】

【発明の効果】本発明によれば、電子認証の確認方法として、ＩＤ、パスワード、鍵といった単一または複数の秘密の正当性を判定する方式に比べ、電子化書類と認証者の電子計算機に分散し多重化された認証情報の整合性を確認する方式は、改竄においては電子化書類と認証者全員の電子計算機の認証情報が対象となり、その冗長性において認証情報の改竄を困難とするとともに、改竄の発見を容易とする。また、電子認証の確認方法として、ＩＤ、パスワード、鍵といった単一または複数の秘密の正当性を判定する方式に比べ、電子化書類と認証者の電子計算機に分散し多重化された認証情報の整合性を確認する方式は、盗用される秘密が存在せず、秘密の盗用による改竄は不可能である。また、電子化書類と認証者の電子計算機に分散し多重化された認証情報の整合性を確認するため、特別な暗号・復合のための機構が不要である。

【図面の簡単な説明】

【図１】本発明の一実施例における電子計算機システムの装置構成を示す図である。

6

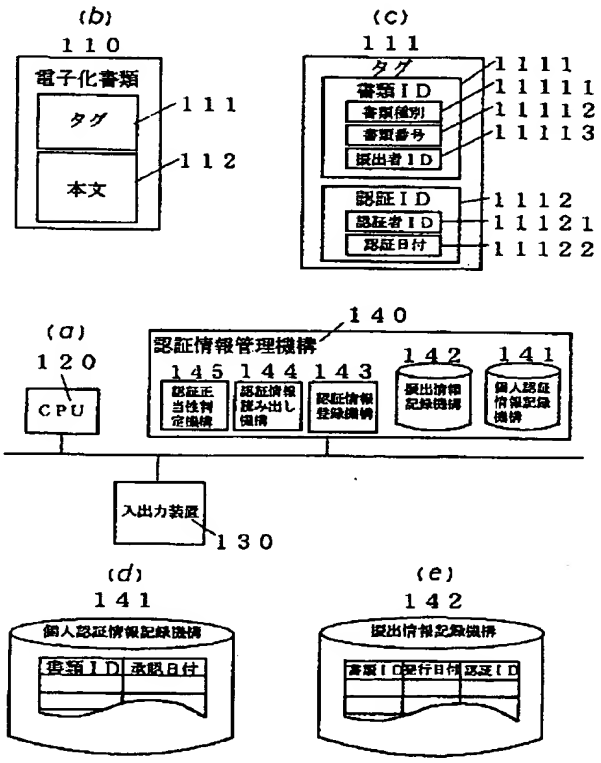
【図２】本発明の一実施例の電子化書類の認証と認証の確認の流れを簡単に示す図である。

【図３】本発明の一実施例の最終判断者の認証正当性確認処理の流れを簡単に示す図である。

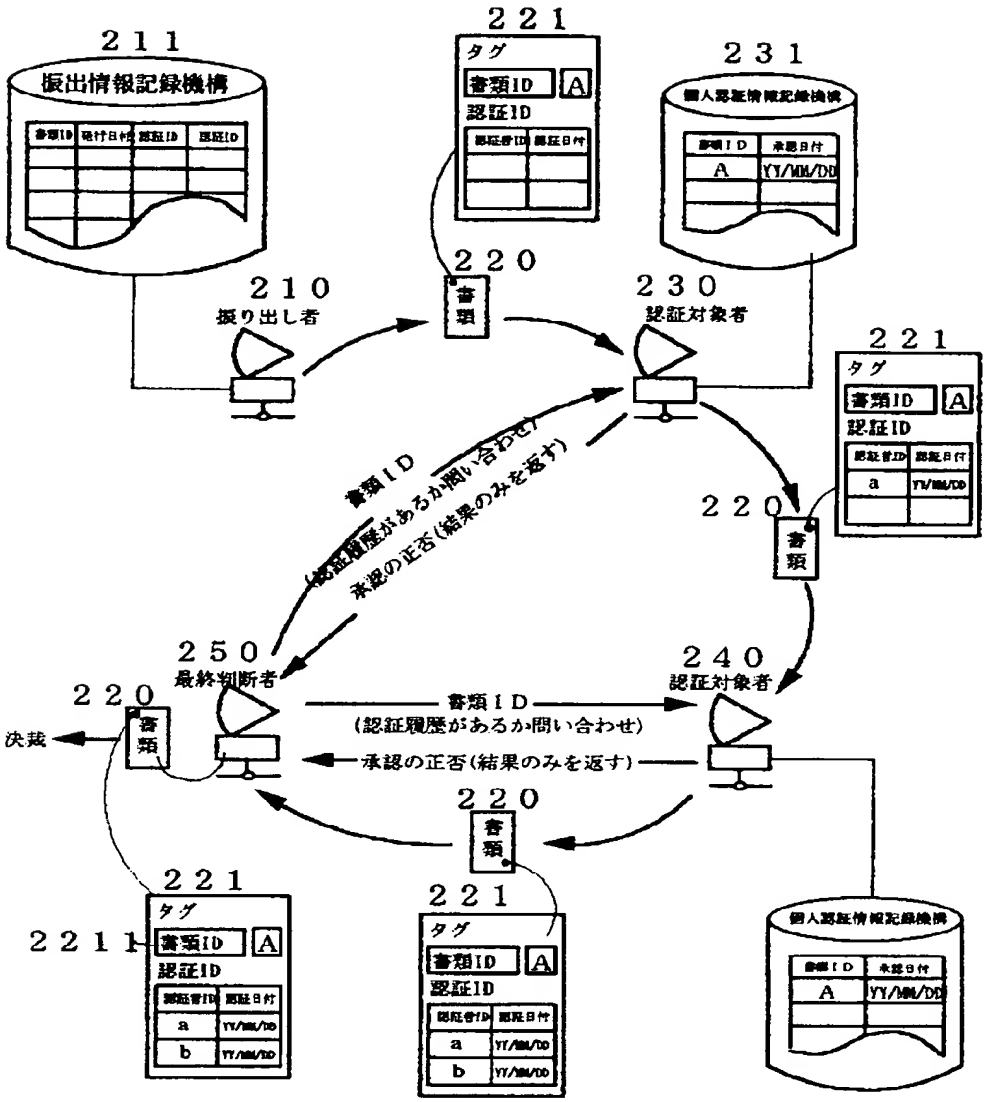
【符号の説明】

１１０：電子化書類、１１１：タグ、１１１１：書類ＩＤ、１１１１１：書類種別、１１１１２：書類番号、１１１１３：振出者ＩＤ、１１１２：認証ＩＤ、１１１２１：認証者ＩＤ、１１１２２：認証日付、１１２：本文、１２：ＣＰＵ、１３０：入出力装置、１４０：認証情報管理機構、１４１：個人認証情報記録機構、１４２：振出情報記録機構、１４３：認証情報登録機構、１４４：認証情報読出機構、１４５：認証正当性判定機構、２１０：振出し者、２１１：振出情報記録機構、２２０：電子化書類、２２１：タグ、２２１１：書類ＩＤ、２３０：認証確認対象者、２３１：個人認証情報記録機構、２４０：認証確認対象者、２５０：最終判断者、３１０：最終判断者、３１１：認証正当性判定機構、３２０：電子化書類、３２１：書類ＩＤ、３３０：認証確認対象者、３３１：認証正当性判定機構、３３２：認証情報読出機構、３３３：個人認証情報記録機構、３３４：メッセージ（承認・不承認）。

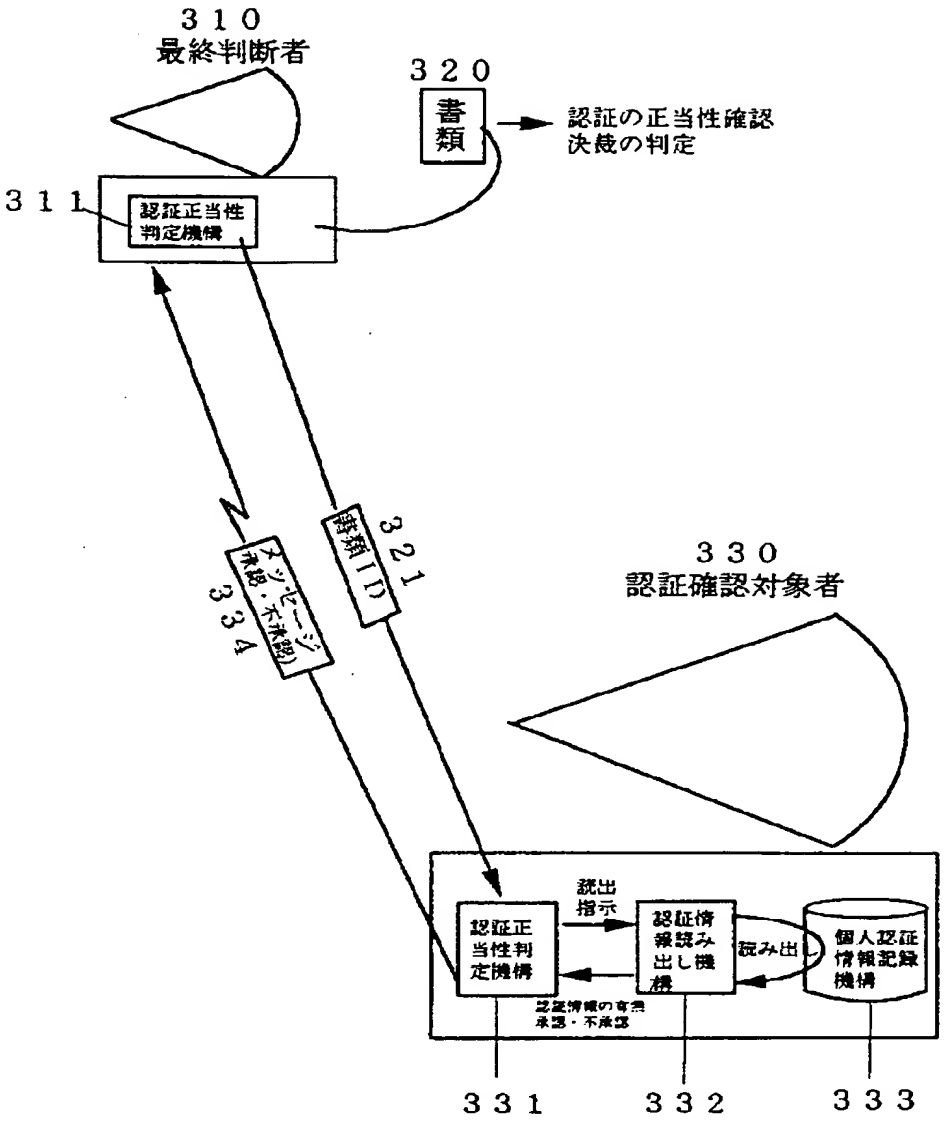
【図１】



【図２】


２１１
振出情報記録機構
２２１
タグ
書類ID
A
認証ID
２３１
個人認証情報記録機構
２２０
書類
２１０
振り出し者
２３０
認証対象者
２２１
タグ
書類ID
A
認証ID
２２０
書類
書類ＩＤ
(認証履歴があるか問い合わせ)
承認の正否(結果のみを返す)
２５０
最終判断者
２４０
認証対象者
２２０
書類
決裁
書類ＩＤ
(認証履歴があるか問い合わせ)
承認の正否(結果のみを返す)
２２０
書類
２２１
タグ
２２１１
書類ID
A
認証ID
２２１
タグ
書類ID
A
認証ID
個人認証情報記録機構

【図３】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	F I		技術表示箇所
Ｇ０９Ｃ	1/00	６６０		Ｇ０６Ｆ	15/22	Ｚ
Ｈ０４Ｌ	9/32				15/30	Ｈ
				Ｈ０４Ｌ	9/00	６７３Ｚ